U.S. Department of Defense tests biometrics on contact and contactless military IDs

After three Common Access Card (CAC)-biometric technology demonstration (TD) projects, the Department of Defense (DoD) is considering moving into phase 2 of a program that could lead to four-million-plus biometric enabled DoD CACs.

But the timeframe is still uncertain. Phase 2, for which vendor support has not yet even been requested, is still on the drawing boards. And once it has begun, it will take more than year to complete, according to Min Chong, Senior Project Manager on the CAC biometrics effort for the DoD Biometrics Management Office (BMO).

PROMISE FULFILLED:
Today's Technological Realities
CTST
2004
April 26-29, 2004
The Washington Convention Center, Washington, D.C.
CLICK HERE TO REGISTER FOR FREE EXHIBIT HALL PASS.
USE CODE D135.

There are still key questions to be answered: Will the biometrics be used on the contact or contactless chip? Will the biometrics be stored and matched on or off the card? One thing for certain is that the next generation CAC will include a 64K contact chip versus the 32K chip on current cards, said Mr. Chong. This move will create additional space for the inclusion of biometric templates on the card.

"The DoD CAC-Biometrics Working Group (BWG) was tasked to explore the inclusion of biometrics technology on the CAC and provide a recommendation to the DOD Smart Card Senior Coordinating Group on how biometrics should be utilized with the next generation CAC card," added Mr. Chong. The next generation CAC will have a 64K chip but the incorporation of the contactless capability will be determined at a later date.

The reason is simple. "When you add more functionality, the card becomes more expensive," said Mr. Chong. "The key stakeholders will want to know what the requirements are and what kind of return they can expect on their investment."

The three TDs were performed during the past two years. The first TD explored using biometrics to open the CAC in lieu of, or as an alternative to a PIN. The second TD examined using biometrics stored on a CAC for logical and physical access. The third looked at using the contactless technology with biometrics, explained Mr. Chong.

Here is a more detailed breakdown of each project, as provided by Mr. Chong:

CAC-A

The first project, referred to as CAC-A, focused on the development of four-scenario proof-of-concept designs to accommodate three different types of DoD users. Each design used biometrics in addition to, or as an alternative to, but not as a replacement for the PIN. Phase I consisted of two distinct parts. Part 1 of Phase I solicited contractor teams to develop biometric technology solutions to satisfy the requirements of four demonstration scenarios:

Scenario 1: Store biometric template on the server and perform match operations on the server. This is designed for the desktop PC.

Scenario 2: Store biometric template on the workstation and perform match operations on the workstation. This scenario is designed to meet the needs of the mobile DoD user.

more >>

Scenario 3: Store biometric template on the CAC and perform the match operation on the server. This is designed for a DoD user who needs to securely transport his or her biometric to multiple sites and use it in both physical and logical network systems.

Scenario 4: Store a biometric template on the CAC and perform the match operation on the CAC. This is designed to meet the needs of both users identified in Scenarios 1 and 2 but never require the passing of biometric information outside of the CAC or middleware.

Part 2 of Phase I was an effort to develop an applet that supports a generic/non-proprietary PIN/key (buffer) solution for the CAC. The Defense Manpower Data Center (DMDC)-West was responsible for Part 2 of Phase I and is currently developing a new Access Control Applet (ACA) with a biometric plug-in capability.

CAC-B

The second demonstration project, called CAC-B, was a continuation of CAC-A Scenario 3 in which the biometrics template was stored on the CAC and the match operation was performed on the server. This effort used the CAC as a transport device for a biometric template. The purpose of the CAC-B technology demonstration was to demonstrate the use of a Biometric Attribute Certificate on the CAC and test its functionality in both physical and logical access environments. Also, the CAC-B utilized a digitally signed biometric template along with other information that allowed revocation and assurance provided by the X.509 standards and format.

CAC-C

CAC-C, the third demonstration project, focused on the use of biometrics with contactless technology. The goal of CAC-C was to provide the DoD community an open and interoperable contactless physical security solution that uses biometrics as an authentication mechanism for a physical access system, a portable physical access system, and a physical access system utilizing a turnstile. CAC-C demonstrated five scenarios with each scenario employing both Mifare and DESFire contactless technologies.

Scenario 1A:
Store biometric template at reader, match at reader.

Scenario 1B Stationary:
Standalone biometric reader, match at reader.

Scenario 1B Mobile:
Mobile biometric reader, match at reader.

Scenario 2:
Store template on contactless chip, match at reader.

Scenario 3:
Store template on control panel, match at control panel.

BearingPoint coordinates the projects

The prime contractor for CAC-A, CAC-B, and CAC-C was BearingPoint Inc. Company representatives would not comment on the results of the demonstration projects. Mr. Chong indicated that none of the results were currently publicly available.

However, a press release distributed by BearingPoint when it was awarded the third contract a year ago, pointed out that the company was able to demonstrate "that a biometric can be securely stored and/or matched on the server, the client, or the CAC. The second contract," the release went on, "successfully demonstrated the use of a smart card paired with a biometric to replace a user name and password to securely log on to applications such as the Microsoft Windows 2000 Active Directory Network and other secure web sites."

more >>

The company's team members on the project included: SPYRUS, Inc., SAFLINK Corp., Precise Biometrics, Xtec, NetVersant, and Datastrip.

Phase II yet to begin

When the project moves into the second phase, said Mr. Chong, CAC-A and CAC-B Phase II efforts will be merged into one effort with two distinct parts.

Part 1:
Concept Refinement will focus on the two distinct possible CAC-Biometric capabilities, the Match-On-Card vs. Match-Off-Card. "This," said Mr. Chong, "requires further analysis and studies to determine if the inclusion of biometric technology on the CAC provides a secure, accurate, convenient, and cost effective authentication mechanism for DoD."

Part 2, he added," will build on CAC-Biometric Phase I results and lessons learned to develop a prototype capability that reflects the optimized results to attain a potential CAC-Biometric solution for the DoD. The BWG will provide an assessment of each of its recommendations in terms of availability of biometric standards."

In essence, "we first wanted to prove that we could use biometrics with the CAC," said Mr. Chong. " Phase 2, not initiated yet, will determine how we would incorporate the biometrics technology with the next generation CAC."

Undecided yet, he added, is which biometric will be used. All types of biometrics–facial, retina scans, but "primarily fingerprints"–were tested in the demonstration projects.

Concludes Mr. Chong, "based on the findings from Part 1, we would build a prototype for Part 2, simulating what the real system would look like–the card specs, the databases, everything. This entire process would take another year."